

Office of Information Technology
1917 Vulnerability and Risk Assessment

2024-10-28

Table of Contents

Policy	2
Authority.....	3
References	4
Applicability.....	5
Definitions	6
Responsibilities	7
RA-1 Risk Assessment Procedures	7
RA-3 Risk Assessment	7
RA-5 Vulnerability Scanning.....	7
History.....	9
Evaluation	10



**Department of Human Services
Online Directives Information System**

Index: POL1917

Revised: 03/20/2024

Next Review: 03/20/2026

Subject: DHS Information Security Policies

Policy

This policy establishes the Enterprise Risk Management Policy, for managing risk associated with information assets, information leakage, and network vulnerabilities. The Risk Management Policy and associated plans, augment DHS mission, by proactively identifying threats and vulnerabilities, which can result in consequences (impact).

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services
5. Georgia Technology Authority

References

- [United States Department of Commerce National Institute for Standards and Technology \(NIST\) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015](#)
- [United States Department of Commerce National Institute for Standards and Technology \(NIST\) Special Publication 800-39 “Managing Information Security Risk: Organization, Mission, and Information System View” March 2011](#)
- [United States Department of Commerce National Institute for Standards and Technology \(NIST\) Special Publication 800-115 “Technical Guide to Information Security Testing and Assessment” September 2008](#)
- [Georgia Technology Authority Enterprise Information Security Policy](#)
- [Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges](#)

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

Vulnerability

A hardware, software, or firmware weakness, or design deficiency, that leaves a system open to assault, harm, or unauthorized exploitation, either externally or internally, thereby resulting in unacceptable risk of information compromise, information alteration, or service denial.

Risk Assessment

The identification, evaluation, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk.

Responsibilities

DHS shall adopt the Risk Management principles established in NIST SP 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems,” as the official policy for this domain. The following subsections outline the Risk Management standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

RA-1 Risk Assessment Procedures

DHS shall:

1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for assessing risks to IT resources and information systems on the basis of business and security requirements.
2. Periodic reviews of this policy shall be performed and documented at least within every **three years**, or when there is a **significant change**.
3. Periodic review of vulnerability and risk assessment procedures shall be performed at least **annually**.

RA-3 Risk Assessment

1. Conduct a risk assessment (RA) to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits. The responsibility for conducting the assessment on a period basis is formally assigned to the DHS CISO and/or appointed DHS Information Security management personnel.
2. Document the risk assessment results in a Risk Assessment Report.
3. Review the risk assessment results at least **annually**.
4. Disseminate risk assessment results to designated agency officials.
5. Update the Risk Assessment Report at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions affecting the security state of the system.

RA-5 Vulnerability Scanning

1. Conduct vulnerability scans on the information system and hosted applications at least **monthly** and when new vulnerabilities potentially affecting the system/applications are identified and reported.
2. Employ enterprise vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that:
 - a. Enumerating platforms, software flaws, and improper configurations

- b. Formatting checklists and test procedures.
 - c. Measuring vulnerability impact.
3. Analyzes vulnerability scan reports and results from security control assessments.
 4. Remediate legitimate vulnerabilities based on the organizational assessment of risk.
 5. Share the information obtained from the vulnerability scanning process and security control assessments with SOs and ISOs throughout the GETS environment to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).

History

None

Evaluation

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.